IN THE CLAIMS:

Please AMEND Claims 1 and 9 as follows.

1. (Currently Amended) A method for facilitating access to messages, <u>the method</u> comprising steps of:

storing a message in a <u>common storage area of a</u> database <u>together with all other</u> <u>messages stored in the database, such that all messages are stored in the common storage</u> <u>area</u>;

associating the message with an intended recipient by a first identifier;

notifying the intended recipient using a notification message of the message stored in the database, wherein the notification message contains an address of or a link to a website;

providing the website for the intended recipient to view the message;

authenticating the intended recipient using a second identifier associated with the intended recipient;

searching the database to find messages for the intended recipient by matching the first identifier; and

displaying the message for the intended recipient,

wherein if there is no second identifier associated with the intended recipient, the intended recipient is prompted to create or register a second identifier.

2. (Previously Presented) The method of claim 1, wherein the first identifier is an account number.

3. (Previously Presented) The method of claim 1, wherein the second identifier is a combination of a user identification and password.

4. (Previously Presented) The method of claim 1, wherein the second identifier is a physical characteristic of the intended recipient identifiable by a biometric identification system.

5. (Previously Presented) The method of claim 1, wherein the message includes:

a message portion; and

an attachment file in a format that is different from a format of the message portion.

6. (Previously Presented) The method of claim 1, further comprising a step of encrypting the website to view messages using an encryption method.

7. (Previously Presented) The method of claim 6, wherein the encryption method is SSL.

8. (Cancelled)

9. (Currently Amended) A method for a business to provide customer access to a private message, the method comprising steps of:

storing ~~at least one~~ a private message in a common storage area of a secure database together with all other messages stored in the secure database, such that all messages are stored in the common storage area;

associating the private message with a first identifier corresponding to an intended customer recipient, wherein the first identifier includes an account number;

notifying the intended customer recipient by electronic mail of the private message stored in the secure database, wherein the electronic mail contains an address of or a link to a secure website;

providing the secure website for the intended customer recipient to view the private message;

authenticating the intended customer recipient to view the private message at the secure website using a second identifier associated with the intended customer recipient;

searching the secure database for the first identifier to find the private message to be viewed by the intended customer recipient; and

displaying the private message associated with the intended customer recipient,

wherein if there is no second identifier associated with the intended customer recipient, the intended customer recipient is prompted to create or register a second identifier.

10. (Previously Presented) The method of claim 9, wherein the private message includes at least one of customer account information, a financial statement, a special offer, a response to an inquiry, and a transaction confirmation.

11. (Previously Presented) The method of claim 9, wherein the second identifier includes a physical characteristic of the intended customer recipient identifiable through a biometric identification system.

12. (Previously Presented) The method of claim 9, wherein the private message includes:

a message portion; and

an attachment file in a format that is different from a format of the message portion.

13. (Previously Presented) The method of claim 9, further comprising a step of encrypting the website to view messages using an encryption method.

14. (Previously Presented) The method of claim 13, wherein the encryption method is SSL.

15. (Previously Presented) The method of claim 1, further comprising a step of providing a second address of or link to a secure webpage on the secure website, the secure webpage containing the message, after successfully authenticating the intended recipient.

16. (Previously Presented) The method of claim 1, wherein if the message has multiple intended recipients, a separate copy of the message is not stored in the database for each intended recipient.

17. (Previously Presented) The method of claim 9, wherein the second identifier is at least one of a user identification, an email address, and a password.

18. (Previously Presented) The method of claim 9, further comprising a step of providing a second address of or link to a secure webpage on the secure website, the secure webpage containing the private message, after successfully authenticating the intended customer recipient.

19. (Previously Presented) The method of claim 9, wherein if the private message has multiple intended customer recipients, a separate copy of the private message is not stored in the database for each intended customer recipient.